

LITE DEPALMA GREENBERG & AFANADOR, LLC

Joseph J. DePalma
Jeremy Nash
570 Broad Street Suite 1201
Newark, NJ 07102
Telephone: (973) 623-3000
Facsimile: (973) 623-0858
jdepalma@litedepalma.com
jnash@litedepalma.com

**UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY**

JOSE PALOMINO and JESSICA TUCK, individually and on behalf of all others similarly situated,	:	Civil Action No:
	:	
	:	
<i>Plaintiffs,</i>	:	CLASS ACTION COMPLAINT
	:	
v.	:	JURY TRIAL DEMANDED
	:	
T-MOBILE USA, INC.,	:	
	:	
<i>Defendant.</i>	:	
	:	

Plaintiffs Jose Palomino and Jessica Tuck (“Plaintiffs”), individually and on behalf of all others similarly situated, bring this class action against T-Mobile USA, Inc. (“T-Mobile” or the “Defendant”). Plaintiffs make the following allegations, except as to allegations specifically pertaining to Plaintiffs, upon information and belief based upon, *inter alia*, the investigation of counsel, and review of public documents.

NATURE OF THE ACTION

1. Plaintiffs bring this class action on behalf of a Nationwide Class and a New Jersey Sub-Class (together, the “Classes”) against Defendant because of its failure to protect the confidential personally identifying information of millions of customers—including first and last names, dates of birth, Social Security Numbers, drivers’ license numbers, physical addresses,

phone numbers, T-Mobile account PINs, unique International Mobile Equipment Identity (or “IMEI”) numbers, and unique International Mobile Subscriber Identity (or “IMSI”) numbers (collectively, their “Personally Identifiable Information”). Defendant’s wrongful disclosure has harmed Plaintiffs and the Classes, which includes at least 50 million people.

JURISDICTION AND VENUE

2. This Court has subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d) in that: (1) this is a class action involving more than 1,000 class members; (2) minimal diversity is present as Plaintiffs are citizens of New Jersey (and the proposed class members are from various states) while Defendant is a citizen of Delaware and Washington; and (3) the amount in controversy exceeds the sum of \$5,000,000, exclusive of interest and costs.

3. This Court has personal jurisdiction over Defendant because it does business in and throughout New Jersey; the wrongful acts alleged in this Complaint were committed in New Jersey, among other venues; and Defendant has intentionally availed itself of this jurisdiction by marketing and selling its products and services in New Jersey.

4. Venue is proper in this District pursuant to: (1) 28 U.S.C. § 1391(b)(2) in that a substantial part of the events or omissions giving rise to Plaintiffs’ claims occurred in this District, and 28 U.S.C. § 1391(d) because the transactions giving rise to Plaintiffs’ claims occurred in Jersey City and Orange, New Jersey; and (2) 28 U.S.C. § 1391(b)(3) in that Defendant is subject to personal jurisdiction in this District.

PARTIES

Plaintiff Jose Palomino

5. Plaintiff Jose Palomino is an individual T-Mobile customer residing in Jersey City, New Jersey. His Personally Identifiable Information was compromised in the data breach described herein.

6. At the time of opening his cellular account with T-Mobile, over a decade ago, Plaintiff Palomino was required to provide, among other things, his Social Security Number, driver's license number, first and last name, and physical address.

7. On or about August 16, 2021, Plaintiff Palomino, and the public, was first notified of the data breach by T-Mobile and that cybercriminals had illegally accessed and stolen confidential customer data from millions of T-Mobile customers' accounts. In addition, Plaintiff Palomino received an August 20th text message from T-Mobile notifying him that his Personally Identifiable Information was among the confidential data that cybercriminals illegally accessed and stole from T-Mobile's servers.

8. As a direct and proximate result of the breach, Plaintiff Palomino has made reasonable efforts to mitigate the impact of the breach, including but not limited to: conducting research concerning this data breach; discussing the breach with his family; and researching credit monitoring and identity theft protection services offered by T-Mobile. This is valuable time Plaintiff Palomino otherwise could have spent on other activities.

9. Plaintiff Palomino is very concerned about identity theft and banking fraud, as well as the consequences of such identity theft and fraud resulting from the data breach.

10. Plaintiff Palomino suffered actual injury from having his Personally Identifiable Information compromised as a result of the data breach including, but not limited to (a) damage to and diminution in the value of his Personally Identifiable Information, a form of property that T-Mobile obtained from Plaintiff Palomino; (b) violation of Plaintiff's privacy rights; and (c) present and increased risk arising from the identity theft and fraud.

11. Plaintiff Palomino has and will spend a significant amount of time responding to the impacts of the data breach. The time spent dealing with the fallout from the data breach is time Plaintiff otherwise would have spent on other activities.

12. As a result of the data breach, Plaintiff Palomino anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the data breach. As a result of the data breach, Plaintiff is and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Jessica Tuck

13. Plaintiff Jessica Tuck is an individual T-Mobile customer residing in Orange, New Jersey. Her Personally Identifiable Information was compromised in the data breach described herein.

14. At the time of opening her cellular account with T-Mobile, over a decade ago, Plaintiff Tuck was required to provide, among other things, her Social Security Number, driver's license number, first and last name, and physical address.

15. On or about August 16, 2021, Plaintiff Tuck, and the public, was first notified of the data breach by T-Mobile and that cybercriminals had illegally accessed and stolen confidential customer data from millions of T-Mobile customers' accounts. In addition, Plaintiff Tuck received an August 19 text message from T-Mobile notifying her that her Personally Identifiable Information was among the confidential data that cybercriminals illegally accessed and stole from T-Mobile's servers.

16. As a direct and proximate result of the breach, Plaintiff Tuck has made reasonable efforts to mitigate the impact of the breach, including but not limited to: conducting research concerning this data breach; discussing the breach with her family; reviewing credit reports and financial account statements for any indication of actual or attempted identity theft or fraud; and researching credit monitoring and identity theft protection services offered by T-Mobile. This is valuable time Plaintiff Tuck otherwise could have spent on other activities.

17. Plaintiff Tuck is very concerned about identity theft and banking fraud, as well as the consequences of such identity theft and fraud resulting from the data breach.

18. Plaintiff Tuck suffered actual injury from having her Personally Identifiable Information compromised as a result of the data breach including, but not limited to (a) damage to and diminution in the value of her Personally Identifiable Information, a form of property that T-Mobile obtained from Plaintiff Tuck; (b) violation of Plaintiff's privacy rights; and (c) present and increased risk arising from the identity theft and fraud.

19. Plaintiff Tuck has and will spend a significant amount of time responding to the impacts of the data breach. The time spent dealing with the fallout from the data breach is time Plaintiff otherwise would have spent on other activities.

20. As a result of the data breach, Plaintiff Tuck anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the data breach. As a result of the data breach, Plaintiff is and will continue to be at increased risk of identity theft and fraud for years to come.

Defendant T-Mobile USA, Inc.

21. Defendant T-Mobile USA, Inc. is a Delaware corporation with its principal place of business in Bellevue, Washington.

FACTUAL BACKGROUND

The T-Mobile Data Breach

22. T-Mobile is a nationwide telecommunications company that provides wireless voice, messaging, and data services in the United States, Puerto Rico and the U.S. Virgin Islands under the "T-Mobile" and "Metro by T-Mobile brands." T-Mobile has over 100 million customers and annual revenues of more than \$68 billion.

23. Plaintiffs and other proposed Class Members were required, as current or prospective customers of T-Mobile, to provide T-Mobile with sensitive Personally Identifiable Information to apply for or receive T-Mobile’s wireless voice, messaging, and data services.

24. On August 15, 2021, the Internet news site Vice.com first reported that T-Mobile had suffered a serious data breach. According to the article, a hacker posted to an online forum claiming to have obtained “data related to over 100 million people,” which data “came from T-Mobile servers.”¹ According to the article, the hacker was attempting to sell that data.

25. On the following day, August 16, 2021, T-Mobile publicly admitted that “unauthorized access to some T-Mobile data occurred.” But T-Mobile stated that it had “not yet determined that there [was] any personal data involved.”²

26. T-Mobile did not state when the unauthorized access occurred. But upon information and belief, T-Mobile learned of the breach not through its own proactive and protective cybersecurity systems, but rather because of the report of the hacker attempting to sell the data.

27. T-Mobile’s August 16, 2021 release further stated that T-Mobile was “confident that the entry point used to gain access has been closed.”³ The fact that T-Mobile purports to have quickly located and closed the entry point suggests that, with proper precautions, T-Mobile could have eliminated the threat before the Data Breach occurred and thus prevented the theft of its customers’ Personally Identifiable Information.

¹ Joseph Cox, T-Mobile Investigating Claims of Massive Customer Data Breach, Motherboard: Tech by Vice (Aug. 15, 2021), <https://www.vice.com/en/article/akg8wg/tmobile-investigating-customer-data-breach-100-million> (last visited Sept. 1, 2021).

² T-Mobile Cybersecurity Incident Update (Aug. 16, 2021), <https://www.t-mobile.com/news/network/cybersecurity-incident-update-august-2021> (last visited Sept. 1, 2021).

³ *Id.*

28. The following day, August 17, T-Mobile issued a further public statement admitting that data containing personal information had been stolen from its system. The information included that of “approximately 7.8 million current T-Mobile postpaid customer accounts . . . as well as just over 40 million records of former or prospective customers who had previously applied for credit with T-Mobile.”⁴ The announcement further stated that “approximately 850,000 active T-Mobile prepaid customer names, phone numbers and account PINs were exposed,” and that “similar information from additional inactive prepaid accounts was also accessed.”

29. Then, on August 20, 2021, T-Mobile issued a further release, adding that it had “identified an additional 667,000 accounts of former T-Mobile customers that were accessed with customer names, phone numbers, addresses and dates of birth compromised.”⁵ The release further revealed that “up to 52,000 names related to current Metro by T-Mobile accounts may have been included” among the data stolen.⁶

30. Around this time, T-Mobile sent Plaintiff Palomino and, upon information and belief, other members of the proposed class a text message stating:

T-Mobile has determined that unauthorized access to some of your information, or others on your account, has occurred, like name, address, phone number and DOB. Importantly, we have NO information that indicates your SSN, personal financial or payment information, credit/debit card information, account numbers, or account passwords were accessed. We take the protection of our customers seriously. Learn more about practices that keep your account secure and general recommendations for protecting yourself: t-mo.co/Protect

⁴ T-Mobile Shares Additional Information Regarding Ongoing Cyberattack Investigation (Aug. 17, 2021), available at <https://www.t-mobile.com/news/network/additional-information-regarding-2021-cyberattack-investigation> (last visited Sept. 1, 2021).

⁵ T-Mobile Shares Updated Information Regarding Ongoing Investigation into Cyberattack, (update for Aug. 20, 2021), available at <https://www.t-mobile.com/news/network/additional-information-regarding-2021-cyberattack-investigation> (last visited Sept. 1, 2021).

⁶ *Id.*

Plaintiff Tuck received a similar message from T-Mobile around the same time:

T-Mobile has determined that unauthorized access to some of your personal data has occurred. We have no evidence that your debit/credit card information was compromised. We take the protection of our customers seriously. We are taking actions to protect your T-Mobile account and we recommend that you take action to protect your credit. Read more here: t-mo.co/Protect

31. T-Mobile had obligations—created by contract, industry standards, common law, and its representations to its customers like Plaintiffs and other Class Members—to keep the compromised Personally Identifiable Information confidential and to protect it from unauthorized disclosures. Plaintiffs and Class Members provided their Personally Identifiable Information to T-Mobile with the understanding that T-Mobile and any business partners to whom T-Mobile disclosed the Personally Identifiable Information would comply with their obligations to keep such information confidential and secure from unauthorized disclosures.

32. Indeed, T-Mobile’s Privacy Policy acknowledges that T-Mobile’s customers “trust T-Mobile to connect [them] to the world everyday” and that they “deserve transparency . . . [and] protection,” and pledges to “help [customers] take action to protect [their] privacy.”⁷ In the Privacy Policy, T-Mobile further promises customers to “use administrative, technical, contractual, and physical safeguards designed to protect [their] data while it is under [TMobile’s] control.”

33. Moreover, the Federal Trade Commission (“FTC”) has established security guidelines and recommendations for businesses that possess their customers’ sensitive personally identifiable information to reduce the likelihood of data breaches.⁸ Among such recommendations are: limiting the sensitive consumer information kept; encrypting sensitive information sent to

⁷ T-Mobile Privacy Notice (effective May 5, 2021), <https://www.t-mobile.com/privacy-center/our-practices/privacy-policy> (last visited Sept. 1, 2021).

⁸ See Federal Trade Commission, Protecting Personal Information: A Guide for Business (Oct. 2016), available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_protecting-personal-information.pdf (last visited Sept. 1, 2021).

third parties or stored on computer networks; and identifying and understanding network vulnerabilities.

34. Defendant's data security obligations and promises were particularly important given the substantial increase in data breaches preceding August 2021, which were widely known to the public and to anyone in the telecommunications industry.

35. Moreover, T-Mobile itself has been particularly aware of the vulnerability of its security systems, having previously suffered four data breaches over the past three years. Specifically, in August 2018, information for two million T-Mobile customers was compromised.⁹ In November 2019, information for one million T-Mobile prepaid customers was compromised.¹⁰ In March 2020, an unknown number of T-Mobile's customers' names, addresses, phone numbers, account numbers, rate plans and features, and billing information was compromised.¹¹ And in early December 2020, T-Mobile discovered that the Personally Identifiable Information of about 200,000 customers was compromised.¹²

36. Additionally, in 2017, a security researcher found a glitch on a T-Mobile website that allowed hackers to access the Personally Identifiable Information of a customer, including his or her email addresses, account numbers, and IMSI numbers, if they knew the customer's phone

⁹ See Alicia Hope, Second Data Breach in 2020 for T-Mobile Exposed Customer and Call-Related Information of 200,000 Subscribers, CPO Magazine (Jan. 11, 2021), available at <https://www.cpomagazine.com/cyber-security/second-data-breach-in-2020-for-t-mobile-exposed-customer-and-call-related-information-of-200000-subscribers/> (last visited Sept. 1, 2021).

¹⁰ *Id.*

¹¹ See T-Mobile's Data Breach Exposes Customer's Data and Financial Information, Security (Mar. 6, 2020), <https://www.securitymagazine.com/articles/91856-t-mobiles-data-breach-exposes-customers-data-and-financial-information> (last visited Sept. 1, 2021).

¹² See Alicia Hope, Second Data Breach in 2020 for T-Mobile Exposed Customer and Call-Related Information of 200,000 Subscribers, CPO Magazine (Jan. 11, 2021), available at <https://www.cpomagazine.com/cyber-security/second-data-breach-in-2020-for-t-mobile-exposed-customer-and-call-related-information-of-200000-subscribers/> (last visited Sept. 1, 2021).

number.¹³ The researcher stated that “T-Mobile has 76 million customers, and an attacker could have ran a script to scrape the data (email, name, billing account number, IMSI number, other numbers under the same account which are usually family members) from all 76 million of these customers to create a searchable database with accurate and up-to-date information of all users.”¹⁴ T-Mobile had no mechanism in place to prevent this type of data breach.

37. Consumers have choices for wireless voice, messaging, and data services and they would not have chosen to provide their Personally Identifiable Information to T-Mobile had they known that the information would be at heightened risk of compromise due to T-Mobile’s lax data security.

38. Defendant’s repeated security failures demonstrate that it failed to honor their duties and promises by not, among other things: maintaining an adequate data security system to reduce the risk of data breaches and cyber-attacks; adequately protecting Plaintiffs’ and the Classes’ Personally Identifiable Information; failing to reasonably limit the sensitive consumer information kept, in violation of FTC recommendations; and failing to encrypt sensitive information sent to third parties or stored on computer networks, in violation of FTC recommendations.

Data Breaches Lead to Identity Theft

39. Plaintiffs and other Class Members have been injured by the disclosure of their Personally Identifiable Information in the Data Breach.

¹³ Lorenzo Franceschi-Bicchieri, T-Mobile Website Allowed Hackers to Access Your Account Data With Just Your Phone Number, Motherboard: Tech by Vice (Oct. 10, 2017), <https://www.vice.com/en/article/wjx3e4/tmobile-website-allowed-hackers-to-access-your-account-data-with-just-your-phone-number> (last accessed Sept. 1, 2021).

¹⁴ *Id.*

40. The United States Government Accountability Office noted in a June 2007 report on Data Breaches (“GAO Report”) that identity thieves use identifying data such as Social Security Numbers to open financial accounts, receive government benefits and incur charges and credit in a person’s name.¹⁵ As the GAO Report states, this type of identity theft is the most harmful because it often takes some time for the victim to become aware of the theft, and the theft can impact the victim’s credit rating adversely.

41. In addition, the GAO Report states that victims of identity theft will face “substantial costs and inconveniences repairing damage to their credit records” and their “good name.”¹⁶

42. Identity theft victims frequently are required to spend many hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen personal information such as social security numbers (“SSNs”) for a variety of crimes, including credit card fraud, phone or utilities fraud, and/or bank/finance fraud.

43. There may be a time lag between when Personally Identifiable Information is stolen and when it is used. According to the GAO Report:

[L]aw enforcement officials told us that in some cases, *stolen data may be held for up to a year or more before being used to commit identity theft*. Further, once stolen data have been sold or posted on the Web, *fraudulent use of that information may continue for years*. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.¹⁷

44. With access to an individual’s Personally Identifiable Information, criminals can do more than just empty a victim’s bank account—they can also commit all manner of fraud,

¹⁵ See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent Is Unknown (June 2007), United States Government Accountability Office, available at <https://www.gao.gov/new.items/d07737.pdf> (last visited Sept. 1, 2021).

¹⁶ *Id.* at 2, 9.

¹⁷ *Id.* at 29 (emphasis supplied).

including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name. Identity thieves may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.¹⁸

45. Personally Identifiable Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, SSNs, and other Personally Identifiable Information directly on various Internet websites making the information publicly available.

CLASS ALLEGATIONS

46. In accordance with Federal Rules of Civil Procedure 23(b)(2) and (b)(3), Plaintiffs bring this case as a class action on behalf of a Nationwide Class and a New Jersey Sub-Class, defined as follows:

Nationwide Class: All persons in the United States whose Personally Identifiable Information was maintained on the T-Mobile systems that were compromised as a result of the breach announced by T-Mobile on or around August 16, 2021.

New Jersey Sub-Class: All persons in the State of New Jersey whose Personally Identifiable Information was maintained on the T-Mobile systems that were compromised as a result of the breach announced by T-Mobile on or around August 16, 2021.

¹⁸ See Federal Trade Commission, Warning Signs of Identity Theft, available at <https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft> (last visited Sept. 1, 2021).

47. The Classes are each so numerous that joinder of all members is impracticable. On information and belief, the Classes each have more than 1,000 members. Moreover, the disposition of the claims of the Classes in a single action will provide substantial benefits to all parties and the Court.

48. There are numerous questions of law and fact common to Plaintiffs and Class Members. These common questions of law and fact include, but are not limited to, the following:

- a. Whether Defendant owed Plaintiffs and other Class Members a duty to implement and maintain reasonable security procedures and practices to protect their Personally Identifiable Information, and whether it breached that duty;
- b. Whether Defendant continues to breach duties to Plaintiffs and the other Class Members;
- c. Whether Defendant's data security systems prior to the Data Breach met industry standards;
- d. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay;
- e. Whether Plaintiffs' and other Class members' Personally Identifiable Information was compromised in the Data Breach; and
- f. Whether Plaintiffs and other Class Members are entitled to damages as a result of Defendant's conduct.

49. Plaintiffs' claims are typical of the claims of the Classes' claims. Plaintiffs suffered the same injury as Class Members—i.e., Plaintiffs' Personally Identifiable Information was compromised in the Data Breach.

50. Plaintiffs will fairly and adequately protect the interests of the Classes. Plaintiffs have retained competent and capable attorneys with significant experience in complex and class action litigation, including data breach class actions. Plaintiffs and their counsel are committed to prosecuting this action vigorously on behalf of the Classes and have the financial resources to do so. Neither Plaintiffs nor their counsel has interests that are contrary to or that conflict with those of the proposed Classes.

51. Defendant has engaged in a common course of conduct toward Plaintiffs and other Class Members. The common issues arising from this conduct that affect Plaintiffs and Class Members predominate over any individual issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

52. A class action is the superior method for the fair and efficient adjudication of this controversy. In this regard, the Class Members' interests in individually controlling the prosecution of separate actions are low given the magnitude, burden, and expense of individual prosecutions against large corporations such as Defendant. It is desirable to concentrate this litigation in this forum to avoid burdening the courts with individual lawsuits. Individualized litigation presents a potential for inconsistent or contradictory judgments, and also increases the delay and expense to all parties and the court system presented by the legal and factual issues of this case. By contrast, the class action procedure here will have no management difficulties. Defendant's records and the records available publicly will easily identify the Class Members. The same common documents and testimony will be used to prove Plaintiffs' claims.

53. A class action is appropriate under Fed. R. Civ. P. 23(b)(2) because Defendant has acted or refused to act on grounds that apply generally to Class Members, so that final injunctive relief or corresponding declaratory relief is appropriate as to all Class Members.

FIRST COUNT
Negligence

54. Plaintiffs reallege and incorporate by reference all preceding factual allegations.

55. T-Mobile required Plaintiffs and Class Members to submit non-public Personally Identifiable Information to obtain its telecommunications services.

56. By collecting and storing this data, and sharing it and using it for commercial gain, Defendant both had a duty of care to use reasonable means to secure and safeguard this Personally Identifiable Information, to prevent disclosure of the information, and to guard the information from theft.

57. Defendant's duty included a responsibility to implement a process by which they could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

58. Defendant also owed a duty of care to Plaintiffs and members of the Classes to provide security consistent with industry standards and the other requirements discussed herein, and to ensure that their systems and networks—and the personnel responsible for them adequately protected their customers' Personally Identifiable Information.

59. Defendant's duty to use reasonable security measures arose as result of the special relationship that existed between it and its customers. Only Defendant was in a position to ensure that its systems were sufficient to protect against the harm to Plaintiffs and the members of the Classes from a data breach.

60. In addition, Defendant had a duty to use reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

61. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the common law, statutes, and FTC guidance described above, but also because they are bound by, and have committed to comply with, industry standards for the protection of confidential Personally Identifiable Information.

62. Defendant breached its common law, statutory and other duties—and thus, were negligent—by failing to use reasonable measures to protect its customers' Personally Identifiable Information, and by failing to provide timely notice of the Data Breach.

63. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- a. failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs' and Class Members' Personally Identifiable Information;
- b. allowing unauthorized access to Plaintiffs' and Class Members' Personally Identifiable Information;
- c. failing to recognize in a timely manner that Plaintiffs' and other Class Members' Personally Identifiable Information had been compromised; and
- d. failing to warn Plaintiffs and other Class Members about the Data Breach in a timely manner so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

64. It was foreseeable that Defendant's failure to use reasonable measures to protect Personally Identifiable Information and to provide timely notice of the Data Breach would result in injury to Plaintiffs and other Class Members. Further, the breach of security, unauthorized access, and resulting injury to Plaintiffs and the members of the Classes were reasonably foreseeable.

65. It was therefore foreseeable that the failure to adequately safeguard Personally Identifiable Information would result in one or more of the following injuries to Plaintiffs and the members of the proposed Classes: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

66. Accordingly, Plaintiff, individually and on behalf of all those similarly situated, seeks an order declaring that Defendant's conduct constitutes negligence and awarding damages in an amount to be determined at trial.

SECOND COUNT
Breach of Implied Contract

67. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

68. When Plaintiffs and Class Members paid money and provided their Personally Identifiable Information to Defendant in exchange for services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to safeguard and protect such information and to timely and accurately notify them if their data had been breached and compromised.

69. Defendant solicited and invited prospective customers to provide their Personally Identifiable Information as part of its regular business practices. These individuals accepted Defendant's offers and provided their Personally Identifiable Information to Defendant. In

entering into such implied contracts, Plaintiffs and the Class Members assumed that Defendant's data security practices and policies were reasonable and consistent with industry standards, and that Defendant would use part of the funds received from Plaintiffs and the Class Members to pay for adequate and reasonable data security practices.

70. Plaintiffs and the Class Members would not have provided and entrusted their Personally Identifiable Information to Defendant in the absence of the implied contract between them and Defendant to keep the information secure.

71. Plaintiffs and the Class Members fully performed their obligations under the implied contracts with Defendant.

72. Defendant breached its implied contracts with Plaintiffs and the Class Members by failing to safeguard and protect their Personally Identifiable Information and by failing to provide timely and accurate notice that their personal information was compromised as a result of a data breach.

73. As a direct and proximate result of Defendant's breaches of its implied contracts, Plaintiffs and the Class Members sustained actual losses and damages as described herein.

THIRD COUNT
Breach of Covenant of Good Faith and Fair Dealing

74. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

75. As described above, when Plaintiffs and the Class Members provided their Personally Identifiable Information to Defendant, they entered into implied contracts in which Defendant agreed to comply with its statutory and common law duties and industry standards to protect Plaintiffs' and Class Members' Personally Identifiable Information and to timely detect and notify them in the event of a data breach.

76. These exchanges constituted an agreement between the parties: Plaintiffs and Class Members were required to provide their Personally Identifiable Information in exchange for products and services provided by Defendant, as well as an implied covenant by Defendant to protect Plaintiffs' and Class Members' Personally Identifiable Information in its possession.

77. It was clear by these exchanges that the parties intended to enter into an agreement. Plaintiffs and Class Members would not have disclosed their Personally Identifiable Information to Defendant but for the prospect of Defendant's promise of certain products and services. Conversely, Defendant presumably would not have taken Plaintiffs' and Class Members' Personally Identifiable Information if it did not intend to provide Plaintiffs and Class Members with the products and services it was offering.

78. Implied in these exchanges was a promise by Defendant to ensure that the Personally Identifiable Information of Plaintiffs and Class Members in its possession was only used to provide the agreed-upon products and services.

79. Plaintiffs and Class Members therefore did not receive the benefit of the bargain with Defendant, because they provided their Personally Identifiable Information in exchange for TMobile's implied agreement to keep it safe and secure.

80. While Defendant had discretion in the specifics of how it met the applicable laws and industry standards, this discretion was governed by an implied covenant of good faith and fair dealing.

81. Defendant breached this implied covenant when it engaged in acts and/or omissions that are declared unfair trade practices by the FTC and state statutes and regulations. These acts and omissions included: omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Plaintiffs' and Class Members' Personally Identifiable Information; storing the Personally Identifiable Information of former customers, despite any valid

purpose for the storage thereof having ceased upon the termination of the business relationship with those individuals; and failing to disclose to Plaintiffs and Class Members at the time they provided their Personally Identifiable Information to it that Defendant's data security systems failed to meet applicable legal and industry standards.

82. Plaintiffs and Class Members did all or substantially all the significant things that the contract required them to do.

83. Likewise, all conditions required for Defendant's performance were met.

84. Defendant's acts and omissions unfairly interfered with Plaintiffs' and Class Members' rights to receive the full benefit of their contracts.

85. Plaintiffs and Class Members have been or will be harmed by Defendant's breach of this implied covenant in the many ways described above, including actual identity theft and/or imminent risk of certainly impending and devastating identity theft that exists now that cyber criminals have their Personally Identifiable Information, and the attendant long-term expense of attempting to mitigate and insure against these risks.

86. Defendant is liable for its breach of these implied covenants, whether or not it is found to have breached any specific express contractual term.

87. Plaintiffs and Class Members are entitled to damages, including compensatory damages and restitution, declaratory and injunctive relief, and attorney fees, costs, and expenses.

FOURTH COUNT **Breach of Confidence**

88. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

89. At all times during Plaintiffs' and Class Members' interactions with Defendant as its customers, Defendant was fully aware of the confidential and sensitive nature of Plaintiffs' and

Class Members' Personally Identifiable Information that Plaintiffs and Class Members provided to Defendant.

90. Plaintiffs' and Class Members' Personally Identifiable Information constitutes confidential and novel information. Indeed, Plaintiffs' and Class Members' Social Security numbers can be changed only with great difficulty and time spent, which still enables a threat actor to exploit that information during the interim; additionally, an individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

91. As alleged herein, Defendant's relationship with Plaintiffs and Class Members was governed by terms and expectations that Plaintiffs' and Class Members' Personally Identifiable Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

92. Plaintiffs and Class Members provided their respective Personally Identifiable Information to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the Personally Identifiable Information to be disseminated to any unauthorized parties.

93. Defendant voluntarily received in confidence Plaintiffs' and Class Members' Personally Identifiable Information with the understanding that the Personally Identifiable Information would not be disclosed or disseminated to the public or any unauthorized third parties.

94. Due to Defendant's failure to prevent, detect, and avoid the Data Breach from occurring by, *inter alia*, not following best information security practices and by not providing proper employee training to secure Plaintiff's and Class Members' Personally Identifiable

Information, Plaintiffs' and Class Members' Personally Identifiable Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and Class Members' confidence, and without their express permission.

95. As a direct and proximate cause of Defendant's actions and omissions, Plaintiffs and Class Members have suffered damages.

96. But for Defendant's disclosure of Plaintiffs' and Class Members' Personally Identifiable Information, in violation of the parties' understanding of confidence, Plaintiffs' and Class Members' Personally Identifiable Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class Members' Personally Identifiable Information, as well as the resulting damages.

97. This disclosure of Plaintiffs' and Class Members' Personally Identifiable Information constituted a violation of Plaintiffs' and Class Members' understanding that Defendant would safeguard and protect the confidential and novel Personally Identifiable Information that Plaintiffs and Class Members were required to disclose to Defendant.

98. The concrete injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs' and Class Members' Personally Identifiable Information. Defendant knew its data security procedures for accepting and securing Plaintiffs' and Class Members' Personally Identifiable Information had numerous security and other vulnerabilities that placed Plaintiffs' and Class Members' Personally Identifiable Information in jeopardy.

99. As a direct and proximate result of Defendant's breaches of confidence, Plaintiffs and Class Members have suffered or are at a substantial risk of suffering concrete injury that includes but is not limited to: (a) actual identity theft; (b) the compromise, publication, or theft of

their Personally Identifiable Information; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Personally Identifiable Information; (d) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (e) the continued risk to their Personally Identifiable Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Personally Identifiable Information in its continued possession; and (f) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

FIFTH COUNT
Invasion of Privacy

100. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

101. Plaintiffs and Class Members had a legitimate and reasonable expectation of privacy with respect to their Personally Identifiable Information and were accordingly entitled to the protection of this personal information against disclosure to and acquisition by unauthorized third parties.

102. Defendant owed a duty to its customers, including Plaintiffs and Class Members, to keep their Personally Identifiable Information private and confidential.

103. The unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, or viewing of Personally Identifiable Information, especially the Personally Identifiable Information that is the subject of this action, is highly offensive to a

reasonable person.

104. This intrusion of privacy was an intrusion into a place or thing belonging to Plaintiffs and Class Members that was private and is entitled to remain private. Plaintiffs and Class Members disclosed their Personally Identifiable Information to Defendant as part of their purchases of Defendant's products and services but did so privately with the intention and understanding that the Personally Identifiable Information would be kept confidential and protected from unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing. Plaintiffs and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization. The Data Breach, which was caused by Defendant's negligent actions and inactions, constitutes an intentional interference with Plaintiffs' and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

105. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

106. Defendant invaded Plaintiff's and Class Members' privacy by failing to adequately implement data security measures, despite its obligations to protect current and former customers' highly sensitive Personally Identifiable Information.

107. Defendant's motives leading to the Data Breach were financially based. In order to save on operating costs, Defendant decided against the implement of adequate data security measures.

108. Defendant's intrusion upon Plaintiffs' and Class Members' privacy in order to save money constitutes an egregious breach of social norms.

109. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and Class Members.

110. As a proximate result of Defendant's acts and omissions, Plaintiffs' and Class Members' Personally Identifiable Information was accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, obtained by, released to, stolen by, used by, or viewed by third parties without authorization, causing Plaintiffs and Class Members to suffer concrete damages as described herein.

111. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that the Personally Identifiable Information maintained by Defendant can still be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, or viewed by unauthorized persons.

112. Plaintiffs and Class Members have no adequate remedy at law for the injuries they have suffered and are at imminent risk of suffering in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and Class Members.

SIXTH COUNT
Misrepresentation

113. Plaintiffs reallege and incorporate by reference each of the allegations set forth above.

114. Defendant falsely represented to Plaintiffs and Class Members that it would take appropriate and reasonable measures to safeguard their Personally Identifiable Information and promptly notify them of a data breach.

115. Plaintiffs and Class members reasonably relied upon said representations in that they provided Defendant their Personally Identifiable Information.

116. Defendant's misrepresentations were material, as Plaintiffs and Class Members would not have chosen to provide their Personally Identifiable Information to T-Mobile had they known that the information would be at heightened risk of compromise due to T-Mobile's lax data security.

117. As a result of Defendant's misrepresentations, Plaintiffs and the Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personally Identifiable Information, and thereby suffered ascertainable economic loss.

SEVENTH COUNT
Violation of the New Jersey Consumer Fraud Act
N.J.S.A. § 56:8-1, *et seq.*

118. Plaintiffs reallege and incorporate by reference each of the allegations set forth above.

119. Plaintiffs and all Class members are "consumers" as that term is defined by the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1.

120. The Defendant is a "person" as that term is defined by the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1(d).

121. Defendant's conduct as alleged herein related to "sales," "offers for sale," or "bailment" as defined by N.J.S.A. 56:8-1.

122. Defendant advertised, offered, or sold goods or services in New Jersey and engaged in trade or commerce directly or indirectly affecting the citizens of the State of New Jersey.

123. Defendant solicited Plaintiffs and Class Members to do business and uniformly and knowingly misrepresented to that by joining, their Personally Identifiable Information was safe,

confidential and protected from intrusion, hacking or theft.

124. Defendant misrepresented that it would protect the privacy and confidentiality of Plaintiff and Class Members' Personally Identifiable Information, including by implementing and maintaining reasonable security measures.

125. Defendant intended to mislead Plaintiffs and Class Members and induce them to rely on their misrepresentations and omissions.

126. Defendant failed to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Class Members' Personally Identifiable Information in violation of N.J.S.A. 56:8-162, which was a direct and proximate cause of the Data Breach.

127. Defendant failed to provide notice to Plaintiffs and Class Members or otherwise comply with the notice requirements of N.J.S.A. 56:8-163.

128. Defendant's acts and omissions, as set forth herein, evidence a lack of good faith, honesty in fact and observance of fair dealing, so as to constitute unconscionable commercial practices, in violation of N.J.S.A. 56:8-2.

129. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiffs and Class Members are required to expend sums to protect and recover their Personally Identifiable Information, have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personally Identifiable Information, and thereby suffered ascertainable economic loss.

130. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including damages, disgorgement, injunctive relief, and attorneys' fees and costs.

EIGHTH COUNT

Violation of the New Jersey Consumer Security Breach Disclosure Act
N.J.S.A. § 56:8-163, *et seq.*

131. Plaintiffs reallege and incorporate by reference each of the allegations set forth above.

132. Under N.J. Stat. Ann. § 56:8-163(a), “[a]ny business that conducts business in New Jersey . . . that compiles or maintains computerized records that include personal information, shall disclose any breach of security of those computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person. The disclosure to a customer shall be made in the most expedient time possible and without unreasonable delay[.]”

133. T-Mobile is a business that conducts business in New Jersey that compiles or maintains computerized records that include personal information under N.J. Stat. Ann. § 56:8-163(a).

134. The Personally Identifiable Information of Plaintiffs and the members of the New Jersey Sub-Class that was compromised in the T-Mobile Breach includes personal information covered under N.J. Stat. Ann. §§ 56:8-163, *et seq.*

135. Because T-Mobile discovered a breach of its security system in which personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured, T-Mobile had an obligation to disclose the T-Mobile Breach in a timely and accurate fashion as mandated under N.J. Stat. Ann. §§ 56:8-163, *et seq.*

136. By failing to disclose the T-Mobile Breach in a timely and accurate manner, T-Mobile violated N.J. Stat. Ann. § 56:8-163(a).

137. As a direct and proximate result of T-Mobile’s violations of N.J. Stat. Ann. § 56:8-163(a), Plaintiffs and the New Jersey Sub-Class members suffered the damages described above.

138. Plaintiffs and the New Jersey Sub-Class members seek relief under N.J. Stat. Ann. § 56:8-19, including but not limited to treble damages (to be proven at trial), attorneys' fees and costs, and injunctive relief.

NINTH COUNT
Declaratory and Injunctive Relief

139. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

140. This Count is brought under the federal Declaratory Judgment Act, 28 U.S.C. §2201.

141. As previously alleged, Plaintiffs and Class Members entered into an implied contract that required Defendant to provide adequate security for the Personally Identifiable Information it collected from Plaintiffs and Class Members.

142. Defendant owes a duty of care to Plaintiffs and Class Members requiring it to adequately secure their Personally Identifiable Information.

143. Defendant still possesses Plaintiffs' and Class Members' Personally Identifiable Information.

144. Since the Data Breach, Defendant has announced few, if any, changes to its data security infrastructure, processes, or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and, thereby, prevent future attacks.

145. Defendant has not satisfied its contractual obligations and legal duties to Plaintiffs and Class Members. In fact, now that Defendant's insufficient data security is known to hackers, the Personally Identifiable Information in Defendant's possession is even more vulnerable to cyberattack.

146. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiffs and Class Members. Further, Plaintiffs and Class Members are at risk of additional or further harm due to the exposure of their Personally Identifiable Information and Defendant's failure to address the security failings that led to such exposure.

147. There is no reason to believe that Defendant's security measures are any more adequate now than they were before the Data Breach to meet Defendant's contractual obligations and legal duties.

148. Plaintiffs, therefore, seek a declaration (1) that Defendant's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

- a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;
- c. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;
- d. Ordering that Defendant segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

- e. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services;
- f. Ordering that Defendant conduct regular computer system scanning and security checks;
- g. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and
- h. Ordering Defendant to meaningfully educate its current, former, and prospective customers about the threats they face as a result of the loss of their Personally Identifiable Information to third parties, as well as the steps they must take to protect themselves.

WHEREFORE, Plaintiffs and Class Members demand judgment as follows:

- A. Certification of the action as a Class Action pursuant to Federal Rule of Civil Procedure 23, and appointment of Plaintiffs as Class Representatives and their counsel of record as Class Counsel;
- B. That acts alleged herein be adjudged and decreed to constitute negligence and violations of the consumer protection laws of New Jersey;
- C. A judgment against Defendant for the damages sustained by Plaintiffs and the Classes defined herein, and for any additional damages, penalties, and other monetary relief provided by applicable law;
- D. An order providing injunctive and other equitable relief as necessary to protect the interests of the Classes, including, but not limited to:

- 1. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks,

penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

2. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

3. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

4. Ordering that Defendant segment consumer data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, unauthorized third parties cannot gain access to other portions of Defendant's systems;

5. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner consumer data not necessary for their provisions of services;

6. Ordering that Defendant conduct regular database scanning and securing checks; and

7. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

E. By awarding Plaintiffs and Class Members pre-judgment and post-judgment interest as provided by law, and that such interest be awarded at the highest legal rate from and after the date of service of the Complaint in this action;

F. The costs of this suit, including reasonable attorney fees; and

G. Such other and further relief as the Court deems just and proper.

JURY TRIAL DEMANDED

Plaintiffs, individually and on behalf of all those similarly situated, hereby request a jury trial, pursuant to Federal Rule of Civil Procedure 38, on any and all claims so triable.

Dated: September 3, 2021

Respectfully submitted,

**LITE DEPALMA GREENBERG
& AFANADOR, LLC**

/s/ Joseph J. DePalma
Joseph J. DePalma
Jeremy Nash
570 Broad Street Suite 1201
Newark, NJ 07102
Telephone: (973) 623-3000
Facsimile: (973) 623-0858
jdepalma@litedepalma.com
jnash@litedepalma.com

Counsel for Plaintiffs and the Classes